CJIS Security Policy Version 5.3, 8/4/2014

What is new and what is on the Horizon

Alan Ferretti
Texas Department of Public Safety
CJIS ISO - Texas

The APB Process

The philosophy underlying the advisory process is one of shared management; that is, the FBI along with local, state, tribal, and federal data providers and system users share responsibility for the operation and management of all systems administered by the FBI for the benefit of the criminal justice community.

Currently, the FBI CJIS Division is responsible for managing the following programs administered by the FBI for the benefit of local, state, tribal, federal, and foreign criminal justice agencies:

- Next Generation Identification (NGI)
- IAFIS
- National Data Exchange (N-DEx)
- Law Enforcement Online (LEO)
- NCIC
- National Instant Criminal Background Check System (NICS)
- UCR

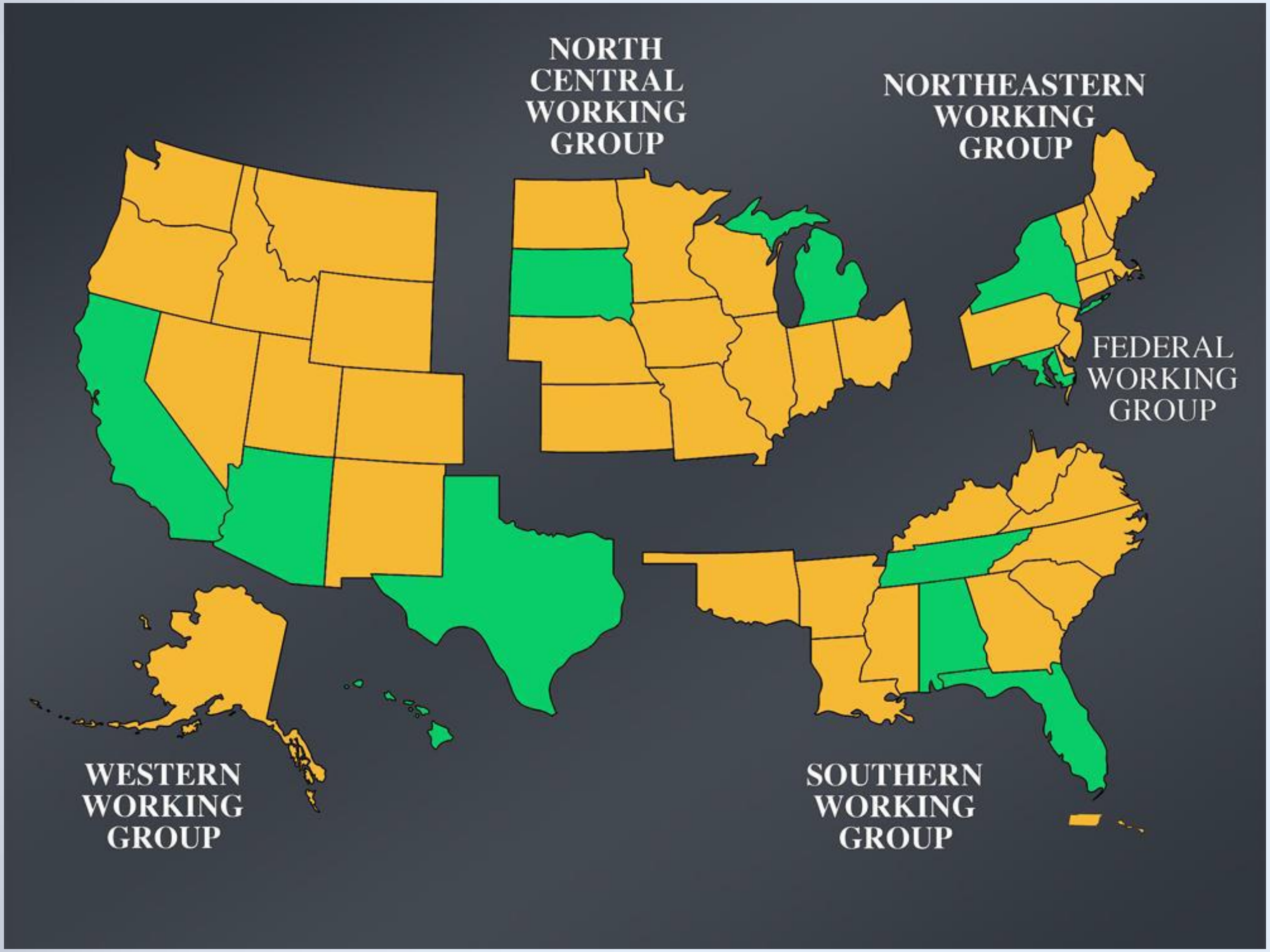
The APB Process

The CJIS Advisory Policy Board (APB)
The APB is composed of 34 representatives from criminal justice agencies and national security agencies and organizations throughout the United States.

The CJIS APB Working Groups
The Working Groups review operational, policy, and technical issues related to CJIS Division programs and policies and make recommendations to the APB or one of its subcommittees. All fifty states, as well as, U.S. territories and the Royal Canadian Mounted Police are organized into five Working Groups

The Security and Access (S+A) Subcommittee
The SA Ad Hoc Subcommittee is responsible for reviewing the hardware and software security policy for current CJIS Division computer systems as well as those systems under development. The Subcommittee recommends to the APB a security policy governing the FBI's CJIS Division systems as well as those systems interfaced with the CJIS Division's computers and telecommunication systems. In addition, this Subcommittee reviews issues related to the requests from agencies and organizations wanting access to information contained in the CJIS Division programs.

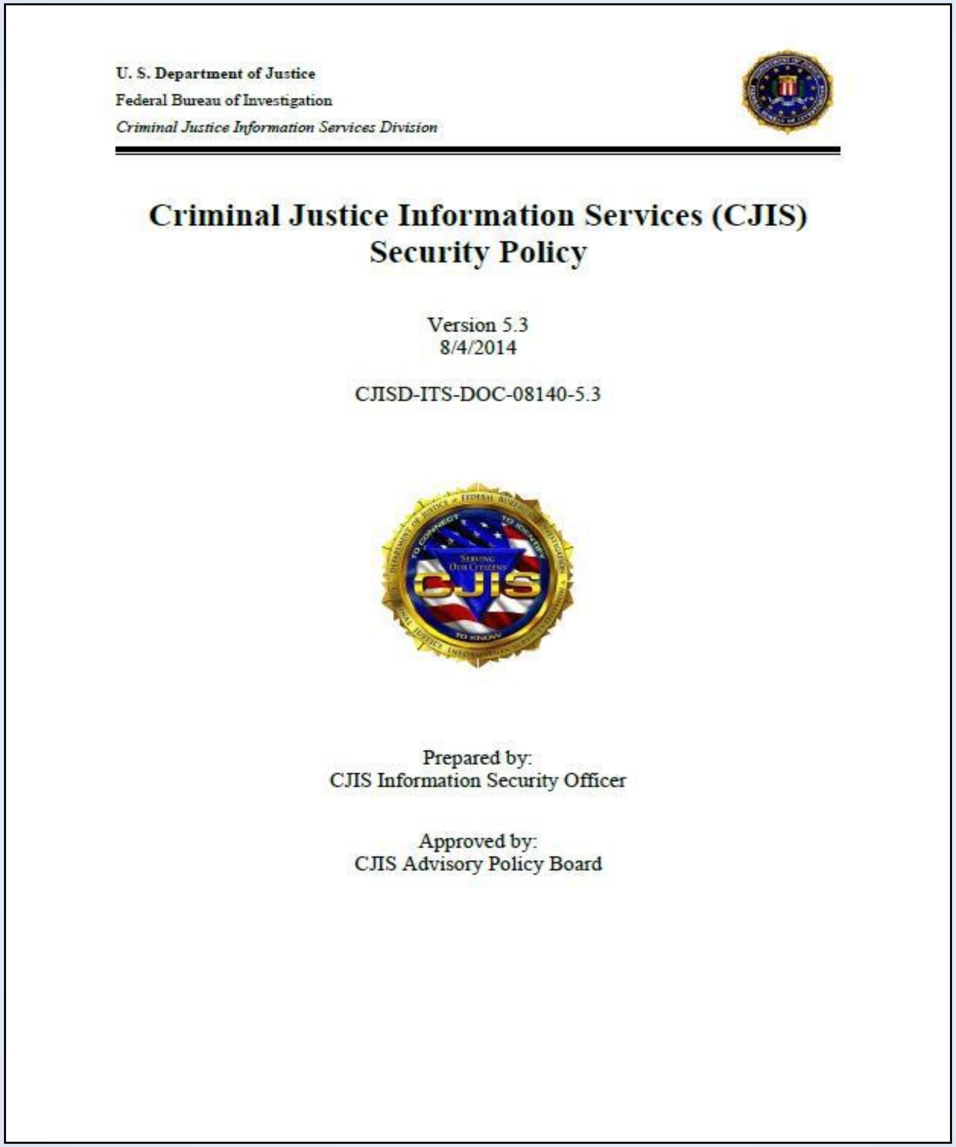
SECURITY AND ACCESS SUBCOMMITTEE



Representation:

Chairman: Alan Ferretti – TX
Vice Chair: Jeff Matthews – AL
Brenda Abaya – HI
Larry Coffee – FL
Joe Dominic – CA
Troy Goodman – MD
Blaine Koops – MI
Yosef Lehrman – NY
Bill Phillips – AZ
Charles Shaffer – FL
TJ Smith – CA
Delton Tipton – SD
Brad Truitt – TN

The Current Version of the CJIS Security Policy



U. S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

Criminal Justice Information Services (CJIS) Security Policy

Version 5.3
8/4/2014

CJISD-ITS-DOC-08140-5.3

Prepared by:
CJIS Information Security Officer

Approved by:
CJIS Advisory Policy Board

Policy Availability

The policy and much associated information is available at either of the following web sites:

The Security Review Web Site (DPS)

http://www.dps.texas.gov/securityreview/

CJIS Security Policy Resource Center (FBI)

http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view

Policy Availability

When to expect a new/changed policy:

- **Annual release cycle**
- **July / August Time Frame**
- **Incorporates APB approved changes from previous year (2 cycles: Spring / Fall)**

What's New in 5.3

- Updated Restricted Files
- Advanced Authentication (Police Vehicles)
- Advanced Authentication (Compensating Controls)
- AA Decision Tree updated
- Indirect Access
- Session Lock Exemption
- Personal Identification Numbers (PIN's)
- CJI at rest encryption exception
- New Policy Area – Section 5.13 Mobile Devices
- Terms and Definitions updated (Appendix A)

Updated Restricted Files

- Section 4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information Updated:

- Add these files:

  Violent Person File

  NICS Denied Transaction File

- Remove this file:

  Immigration Violator File

Advanced Authentication (Police Vehicles)

- Was to expire on Sept. 30, 2014

- For AA purposes, an **<u>ENCLOSED</u>** police vehicle is now a physically secure location

- Devices associated with and located within an enclosed police vehicle do not require Advanced Authentication.

(See Examples)

Secure Locations

NOT Secure Locations (AA required)

Advanced Authentication (Police Vehicles)

Section 5.9.1 Physically Secure Location

“A physically secure location is a facility, ***a police vehicle,*** or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.”

Advanced Authentication (Compensating Controls)

- Addition of ***COMPENSATING CONTROLS*** for AA
- Applies only to smartphones and tablets
- Possession of agency issued device is a required part of control
- Additional requirements mostly met by MDM
- CSO approval and support required

Indirect Access

- Add ***DIRECT or INDIRECT ACCESS*** as a “determiner” for advanced authentication (AA)
- INDIRECT ACCESS - No ability to conduct transactional activities on state and national repositories
- CSO determines whether access is considered indirect

Indirect Access

- Appendix A updated with the definition of ***INDIRECT ACCESS:***

"Having the authority to access systems containing CJI without providing the user the ability to conduct transactional activities (the capability to query or update) on state and national systems (e.g. CJIS Systems Agency (CSA), State Identification Bureau (SIB), or national repositories)."

Session Lock Exemption

- Section 5.5.5 Session Lock

- Modified to include receive-only terminals

"(3) terminals designated solely for the purpose of receiving alert notifications (i.e. receive only terminals or ROT) used within physically secure location facilities that remain staffed when in operation."

Personal Identification Numbers (PIN's)

- Section 5.6.2.1.2 Personal Identification Number

- Addition of PIN requirements
- When used as authenticator must meet password requirements
- Local device authentication – 6 digits
- When used in conjunction with a certificate or token, use the following attributes on the next page………

Personal Identification Numbers (PIN's)

Be a minimum of six (6) digits

Have no repeating digits (i.e., 112233)

Have no sequential patterns (i.e., 123456)

Not be the same as the Userid.

Expire within a maximum of 365 calendar days.

- *If a PIN is used to access a soft certificate which is the second factor of authentication, AND the first factor is a password that complies with the requirements in Section 5.6.2.1.1, then the 365 day expiration requirement can be waived by the CSO.*

Not be identical to the previous three (3) PINs.

Not be transmitted in the clear outside the secure location.
Not be displayed when entered.

EXCEPTION: When a PIN is used for local device authentication, the only requirement is that it be a minimum of six (6) digits.

CJI at rest Encryption Exception

Section 5.10.1.2 Encryption

- Create encryption exception for CJI at rest

"EXCEPTION: When encryption is used for CJI at rest, agencies may use encryption methods that are FIPS 197 certified, AES 256 bit as described on the National Security Agency (NSA) Suite B Cryptography list of approved algorithms."

CJI at rest
Encryption Exception

When agencies implement encryption on CJI at rest, the passphrase used to unlock the cipher shall meet the following requirements:

- *Be at least 10 characters*
- *Not be a dictionary word.*
- *Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character.*
- *Be changed when previously authorized personnel no longer require access.*

New Policy Area – Section 5.13 Mobile Devices

- Consolidation of mobile centric requirements
- Reference to "companion" sections
- Combines previous requirements with new requirements

Mobile Requirements Evolution within S+A

Fall 2011 Security and Access Subcommittee

- *"…creation of a matrix that lists the technology juxtaposed against the requirement."*
- Essentially: Would each device meet the Policy requirements?

Spring 2012 Security and Access Subcommittee

- *"…develop policy language to move towards a BlackBerry Enterprise Server-like standard for mobile devices."*
- BES represents the ideal managed environment with both policy and technical controls

Mobile Requirements Evolution within S+A

Spring 2013 Mobile Security Task Force created

Chaired by Larry Coffee, FL-ISO
Vice-chair Alan Ferretti, TX-ISO

Members comprised of state and local agency mobile SMEs:

Michelle Young, Kent County, MI
Jae Lim, Hawaii Criminal Justice Data Center
Chris DeSain, NY Public Safety
David Painter, Houston, TX PD
Tom Jenkins, Ocala, FL PD

Review topics related to mobile device security and provide recommendations to the S&A Subcommittee

The New Section 5.13 – Mobile Devices

5.13 Section	5.2 Section	Subject
5.13	New	Policy Area 13: Mobile Devices
5.13.1	5.5.7	Wireless Communication Technologies
5.13.1.1	5.5.7.1	All 802.11 Wireless Protocols
5.13.1.2	5.5.7.3	Cellular
5.13.1.3	5.5.7.4	Bluetooth
5.13.2	5.5.7.3.3	Mobile Device Management (MDM)
5.13.3	5.5.7.3.1	Wireless Device Risk Mitigations
5.13.4	New	System Integrity
5.13.4.1	New	Patching/Updates
5.13.4.2	New	Malicious Code Protection
5.13.4.3	New	Physical Protection
5.13.4.4	5.10.4.4	Personal Firewall
5.13.5	New	Incident Response
5.13.6	New	Auditing and Accountability
5.13.7	New	Access Control
5.13.8	New	Wireless Hotspot Capability
5.13.9	New	Identification and Authentication
5.13.9.1	New	Local Device Authentication
5.13.10	New	Device Certificates

Mobile Security

Mobile Security

- What is a Laptop vs Tablet vs Phone?

- Requirements are different, so how do you tell what is what?

Mobile Security

- Is it Form Factor?

Large - vehicle mount or a carrying case and include a monitor with attached keyboard (MDTs/Laptops)

Medium - vehicle mount or portfolio sized carry case that typically consist of a touch screen without attached keyboard (Tablets)

Small - intended for carry in a pocket or 'holster' attached to the body (Smartphones)

Mobile Security

- Is it Operating System?

Full-feature OS – Windows / Linux or Unix / Apple OSX

Limited-feature OS – iOS / Android / BlackBerry

Mobile Security

- Is it Connectivity type?

Cell Only – Always On

WiFi Only – Could include cell “on demand”

Cell Only (always on) plus WiFi “on demand”

+

Mobile Security

Given all the variables involved and the continued evolution, how do we know which set of rules apply to any given device?

Simple solution – look at the box it came in and see what it says.

If the manufacturer classifies it as a Laptop / Tablet / Smart Phone, so will we.

Mobile Security

- Some advice to take away today:
  - Tablets and Smartphones should be under the control of some type of Mobile Device Management, even if the functionality is rudimentary. This is a must-have in a law enforcement environment.
  - WiFi Considerations – Just say no unless absolutely required. Cell service is much more secure.
  - Remember, the target is not the device as much as the backend network and the data that is housed there.
  - No Rooting or Jail-breaking the device. This breaks any inherent security features of the device and voids the warranty.
  - Loss/Theft of small form factor devices is still their most common security issue.

Appendix A Terms and Definitions

- The following have been added to Appendix A:

- Mobile device form factors
  - Pocket/handheld mobile devices
  - Smartphone
  - Tablet Devices
- Indirect Access
- Digital Media
- Receive-only terminal

Texas Security Policy Supplement

- The following has been added:

The Texas Department of Public Safety (DPS), as CJIS Systems Agency (CSA) for the state of Texas, has modified the rules associated with the adjudication of criminal history background checks associated with entities that contract with criminal justice agencies to perform certain aspects of the administration of criminal justice. The specific area of policy change addresses those vendors that provide offsite storage of hard-copy CJI or CJI document destruction as a result of a contract with a criminal justice agency that is subject to a CJIS Security Addendum.

The vendor employees that have this specific hard-copy only access will be held to the standards articulated within the CJIS Security Policy, but will be allowed access to this hard-copy CJI as long as **a felony conviction** of any kind does not exist on the vendor employee's national finger print based record check processed as part of the requirements of the Security Addendum.

The CJIS Security Addendum must be executed with the vendor company and each employee with hard copy access to CJI must sign a Certification page. All other aspects of the CJIS Security Policy must be followed.

Because vendors for this type of service cannot effectuate changes to the source of the CJI, DPS will lessen the CHRI adjudication standard for this group only. Others in the vendor community that support IT efforts, network support, or are under Management Control still must meet the adjudication standard as currently defined by TCOLE.

On The Horizon

- The following changes are either making their way through the process or are being talked about at this point.
- The earliest these would be in the policy is Version 5.4 due out in 2015.
- The following twelve items are not to be considered policy and may never be policy.

On The Horizon

Encryption Exemption
Requirement Tiering
Certificate Use Clarification
Partitioning and Virtualization
Virtual Escorting
In/Out-of-band Clarification
Auditing Facilities in Other Jurisdictions
Policy Area 13: Mobile Devices Update
Mobile Appendix Update
Cloud Appendix Update
Faxing Requirements Update
Appendix K Value

ON THE HORIZON

- Encryption Exemption

Exception to CJIS Security Policy Section 5.10.1.2 Exemptions

Physical or technical controls to allow cabling carrying unencrypted CJI between physically secure locations.

ON THE HORIZON

- Requirement Tiering

Integrating Risk-based Compliance and Requirement Tiering into the CJIS Security Policy

Current Status:

Being presented to the Fall 2014 Working Groups for action

Final stages of determining if and how to integrate requirement tiers into the Policy.

ON THE HORIZON

- Certificate Use Clarification

Current Status: Being presented to the Fall 2014 Working Groups for action

Propose modification to the CJIS Security Policy to clarify the use of certificates, especially in the advanced authentication process.

ON THE HORIZON

- Partitioning and Virtualization

Current Status: Being presented to the Fall 2014 Working Groups for action

Present recommended changes to the Policy to clarify the practice of virtualization and partitioning.

ON THE HORIZON

- Virtualization

Current Status: Being presented to the Fall 2014 Working Groups for action

Identify a method to virtually escort a remote session for system maintenance.

ON THE HORIZON

- In/Out of Band Clarification

- Current Status: Ad Hoc preparation with SA Subcommittee. Planned for Spring 2015 Working Groups for action.

- Add or modify Policy language to clarify the meaning of in/out-of-band use of supplying logon credentials.

ON THE HORIZON

- Auditing Facilities in Other Jurisdictions

Current Status: Topic paper request received and topic being developed for Spring 2015 Working Groups.

This topic will focus on discussing how to modify the CJIS Security Policy to allow a CSA to perform facility inspections of vendors that are in a different state.

ON THE HORIZON

- Policy Area 13 Update

Current Status: Topic paper request submitted by Mobile Security Task Force chairman

During the process to modify the Policy with the mobile updates, a Mobile Security Task Force was created to review mobile-centric topics and provide recommendations to the Security and Access Subcommittee. The task force reviewed the proposed changes and will make recommendations for modifying the Policy.

ON THE HORIZON

- Mobile Appendix Update

Current Status: In development – target Spring 2015
Working Groups

The FBI CJIS ISO Program is developing an update to the Mobile Appendix - bringing the information up to current industry best practices.

ON THE HORIZON

- Cloud Appendix Update

Current Status: Being considered

The FBI CJIS ISO is considering an update to the Cloud Appendix to level the information with current industry best practices.

ON THE HORIZON

- Faxing Requirement Update

Current Status: Draft

Update the language in Section 5.10.2 to keep pace with new fax technology such as fax servers or web based fax services that essentially function as email.

ON THE HORIZON

- Appendix K value

Current Status: Draft

Review Appendix K and determine if it still provides value as a tool to criminal justice agencies with respect to the CJIS Security Policy requirements.

Texas Audit Statistics

- In the 12 months ending August 31, 2014:

There were 67 “new” agencies added for Audit.
Current Total Agencies we audit is 1,227.

Technical Security Auditors Drove 99,310 miles.
There were no accidents (Or speeding tickets)

Completed 436 Technical Audits:
218 were Compliant
124 became Compliant
94 are still working issues

Texas Audit Statistics

- Top Reasons for non-compliance:

  Software, Patches, Updates
  Remote Support - Encryption/AA
  Security Awareness Training
  Local Agency Required Policies

Security Awareness Training

Security Awareness Training

When is Security Awareness Training Required?

- All personnel with access to CJI within six (6) months of initial assignment shall receive training

- Biennially thereafter

Security Awareness Training

- **Three “Levels” of Training (determined by role):**

1. All Personnel (generalized training) – “Level” 1 Only

2. Personnel with Physical and Logical Access (CJI processing) – 1+2

3. Personnel with Information Technology Roles (includes administrator roles) – 1+2+3

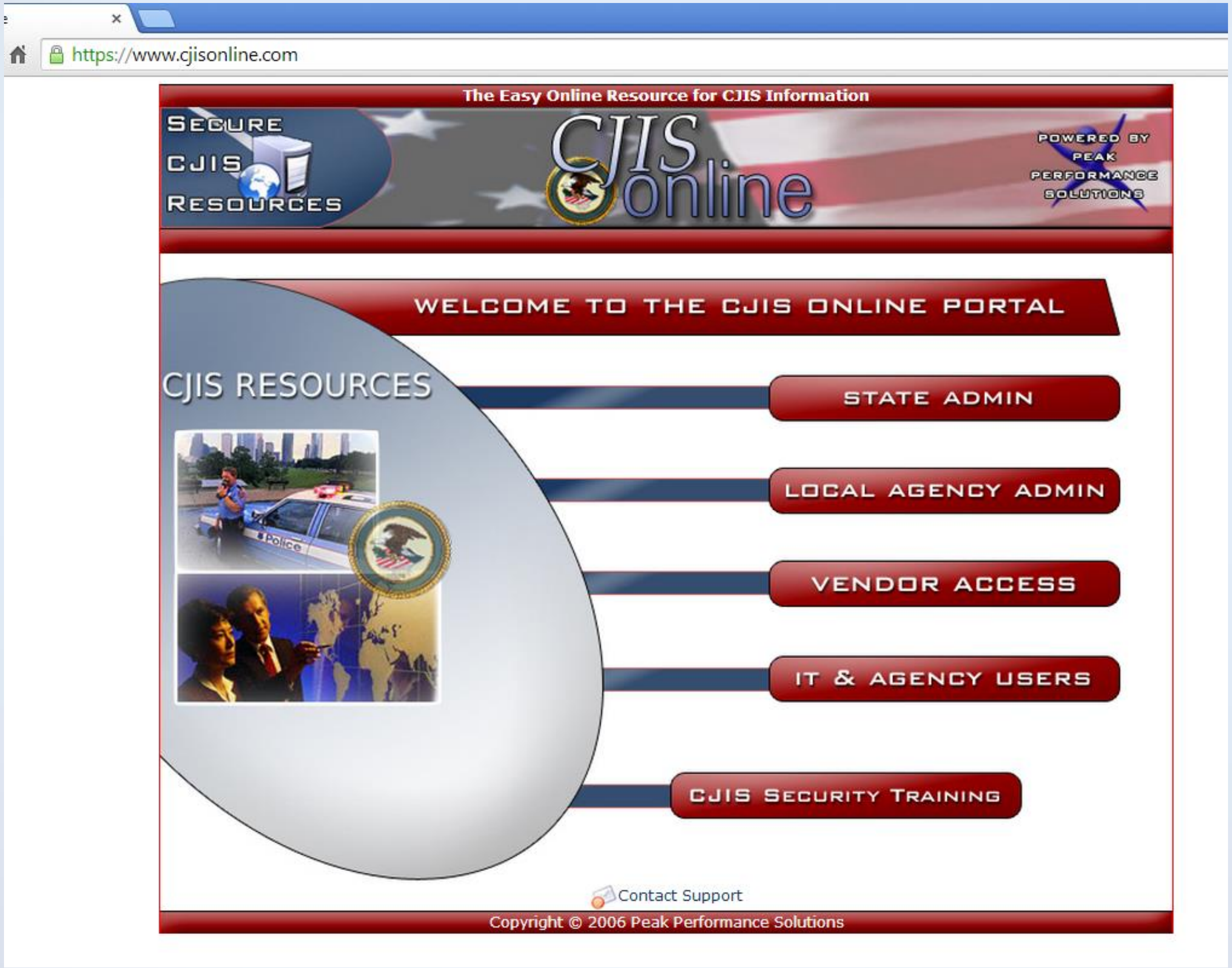
Security Awareness Training

- **The current options for Security Awareness Training are within TLETs (for those with a TLETS ID) or use the DPS provided slide deck (manual tracking) or use your own compliant training (manual tracking).**

This causes duplication of effort across all agencies for Vendors, IT Staff, Support Services, and others.

DPS has purchased and is making available at no charge to agencies a web based application called CJIS Online from Peak Performance.

Security Awareness Training



https://www.cjisonline.com

The Easy Online Resource for CJIS Information

Copyright © 2006 Peak Performance Solutions

Security Awareness Training

Many vendors are pre-loaded into the system. Vendor personnel are only required to take training once. All agencies can track Vendor Status.

IT personnel can be tracked automatically after initial loading into the system.

All 3 levels of training are supported. Can also be used for Agency Support Services.

Administration is done at the local agency level.

Being rolled out to all agencies in Q4 of 2014.

Cloud Computing

Cloud Computing

- **What is Cloud Computing?**

Defined by the CJIS Security Policy as: *A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications, and services), software, and information.*

Cloud Computing

- **Benefits of Cloud Computing**

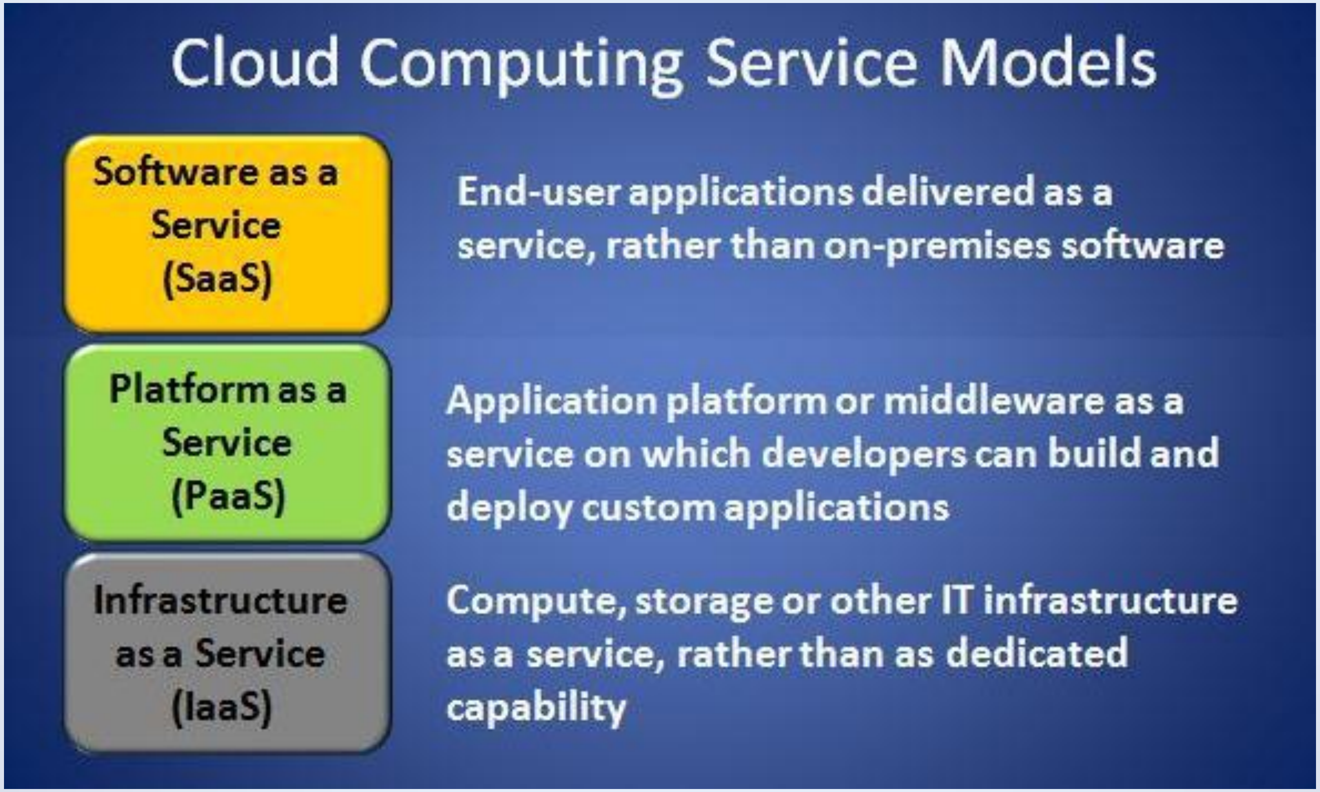
Reduced Budgets

Improved Efficiency

Disaster Recovery

Service Consolidation

Cloud Computing



Cloud Computing Service Models

Software as a Service (SaaS)

End-user applications delivered as a service, rather than on-premises software

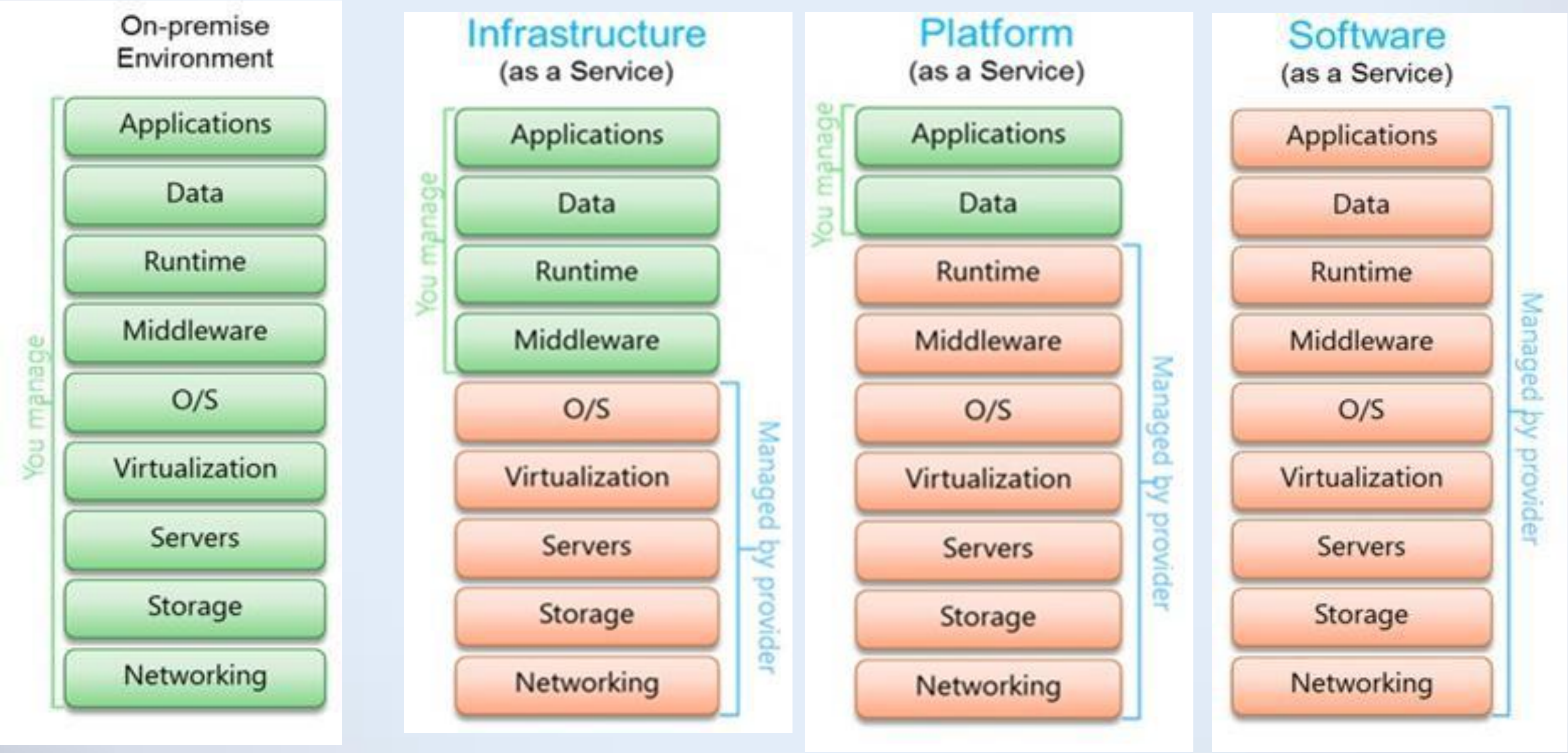
Platform as a Service (PaaS)

Application platform or middleware as a service on which developers can build and deploy custom applications

Infrastructure as a Service (IaaS)

Compute, storage or other IT infrastructure as a service, rather than as dedicated capability

Cloud Computing



On-premise Environment

Applications
Data
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking

You manage

Infrastructure (as a Service)

Applications
Data
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking

You manage

Managed by provider

Platform (as a Service)

Applications
Data
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking

You manage

Managed by provider

Software (as a Service)

Applications
Data
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking

Managed by provider

Cloud Computing

- **Security Concerns with Cloud Computing**

Privileged user access

Regulatory compliance

Data location

Data segregation

Recovery

Investigative support

Long-term viability

Cloud Computing

- **Cloud Computing and the CJIS Security Policy**

Section 5.10.1.5 Cloud Computing

The metadata derived from CJI shall not be used by any cloud service provider for any purposes.

The cloud service provider shall be prohibited from scanning any email or data files for the purpose of building analytics, data mining, advertising, or improving the services provided.

Appendix G.3 Cloud Computing White Paper

The IACP "Guiding Principles on Cloud Computing in Law Enforcement".

Cloud Computing

- **IACP Guiding Principles on Cloud Computing in Law Enforcement.**

1. FBI CJIS Security Policy Compliance
2. Data Ownership
3. Impermissibility of data mining
4. Auditing
5. Portability and interoperability
6. Integrity of Data
7. Survivability of Agreement
8. Confidentiality
9. Availability, Reliability, and Performance
10. Cost- Total Cost of Ownership

Cloud Computing

- **Where are we in Texas**

Google – no interest shown in being compliant. No Change. Encrypt CJI.

Microsoft – Office 365 being used across the State (Country). Microsoft is about to roll out a compliant product, Azure, through DIR, that will allow for cloud based storage of large data files. Same methods as O365 but different data center. Total Government Cloud data centers will be at five.

AWS (Amazon) – had first meeting with DPS regarding CJIS compliance. 8/29/2014. Encrypt CJI.

- Additional Questions:

Alan Ferretti

(512) 424-7186

alan.ferretti@dps.texas.gov

Web Site

www.dps.texas.gov/securityreview

Questions?